COMP 233 Discrete Mathematics

Elementary Number Theory and Methods of Proof

1

Overview

- Direct Proof and Counterexample I:
  - Even and Odd
- Direct Proof and Counterexample II:
  - Rational Numbers
- Direct Proof and Counterexample III:
  - Divisibility and transitivity of divisibility theorem
- Direct Proof and Counterexample IV:
  - Prime numbers and unique factorization theorem
- Proof by Division into cases
  - Quotient-Remainder Theorem
- Proof by contradiction

2

Universal Rules of Inference

The rule of universal instantiation can be combined with any **valid argument form** to obtain the **universal version** of that form

Ex: **Universal Modus ponens**

Modus Ponens
$p \rightarrow q$
p
$\therefore q$

Formal Version
$\forall x$, if $P(x)$ then $Q(x)$. $P(a)$ for a particular a. $\therefore$ $Q(a)$.

Informal Version
If x makes P(x) true, then x makes Q(x) true. a particular element "a" makes P(x) true. ∴ a makes Q(x) true

NOTES!

From now on, we will unconsciously use rules of inference (e.g., modus ponens) at every stage of our proof (التحقق). without specifically stating that ..
We learned it then it became so natural.

Assumptions

-You are familiar with:

- Logic (ch2, ch3)
- Properties of the real numbers (Appendix A)
  - "basic algebra"
  - Properties of equality:

    A = A

    If A = B, then B = A.

    If A = B and B = C, then A = C.
  - Integers are 0, 1, 2, 3, …, -1, -2, -3, …
  - Any sum, difference, or product of integers is an integer.
  - Zero product property
  - Etc.

5

4.1 Direct Proof and Counterexample I: Introduction

How to (dis) prove statements

Before (dis)proving, write a mathematical statement as a Universal or an Existential Statement:

	Proving	Disapproving
$\exists x \in D \ . \ Q(x)$	One example	Negate then direct proof
$\forall x \in D \ . \ Q(x)$	Direct proof	Counter example

This chapter: Direct proofs with numbers

,

Proving Universal Statements

The <u>majority</u> of mathematical statements to be proved are universal.

$$\forall x \in D \ . \ P(x) \rightarrow Q(x)$$

One way to prove such statements is called T**he Method of Exhaustion**, by listing all cases.

Use the method of exhaustion to prove the following:

$\forall n \in Z$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

4 = 2 + 2	6 = 3 + 3	8 = 3 + 5	10 = 5 + 5
12=5+7	14=11+3	16=5+11	18=7+11
20=7+13	22=5+17	24=5+19	26=7+19

➔ **This method** is obviously **impractical**, as we cannot check all possibilities.

Direct Proof Method

Method of Generalizing from the Generic Particular:
If a property can be shown to be true for a particular but arbitrarily chosen element of a set, then it is true for every element of the set.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D, P(x) \rightarrow Q(x)$."
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis P(x) is true. "Suppose $x \in D$ and P(x)"
3. Show that the conclusion Q(x) is true by using
   a. definitions,
   b. previously established results,
   c. rules for logical inference.

Definition of Even and Odd

Notation: ⇔ refers to the universalized "if and only if"

An integer is **even** ⇔ it can be expressed as 2 times some integer.
An integer is **odd** ⇔ it can be expressed as 2 times some integer plus 1.

What it means for a definition to be ⇔:

- If an integer, say *n*, is **even** then ∃ an integer, say *k*, such that $n = 2k$, *AND*
- If an integer, say *n*, can be expressed as $2k$, for some integer *k*, then *n* is **even**.

Think of a definition as a **test**.
***Ex:* Is 0 even?**
Well --- does it pass the test??

Yes!

Examples: Odd & Even

Use the definitions of even and odd to justify your answers to the following questions.

- a. Is 0 even?

  Yes, $0=2\cdot 0$

- b. Is −301 odd?

  Yes, $-301=2(-151)+1$.

- c. If a and b are integers, is $6a^2b$ even?

Yes, $6a^2b = 2(3a^2b)$, and since a and b are integers, so is $3a^2b$ (being a product of integers).

- d. If a and b are integers, is 10a+8b+1 odd?

Yes, $10a+8b+1=2(5a+4b)+1$, and since a and b are integers, so is $5a+4b$ (being a sum of products of integers).

- e. Is every integer either even or odd?

Notes

- Some people say that an integer is **even** if it equals $2k$. Are they right?
- Is 1 an even number?
- Does $1 = 2k$?
- Yes: $1 = 2\cdot(\frac{1}{2})$

So it's pretty important for k to be an integer!

Prime and Composite Numbers

• Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

$$n \text{ is prime} \quad \Leftrightarrow \quad \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite} \quad \Leftrightarrow \quad \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$

- Write the first six prime numbers.
  2, 3, 5, 7, 11, 13
- Write the first six composite numbers
  4, 6, 8, 9, 10, 12

Examples: Prime and Composite Numbers

- Is 1 prime?
  No. A prime number is required to be greater than 1
- Is every integer greater than 1 either prime or composite?

Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely $r = n$ and $s = 1$ and $r = 1$ and $s = n$. Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \le r \le n$ and $1 \le s \le n$. If n is prime, then the two displayed pairs are the only ways to write n as rs. Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

Generalizing from the Generic Particular

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified.

It is called the method of generalizing from the generic particular

Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Trick

▪ Choose any number	5	-7
▪ Double that number	10	-14
▪ Add 12	22	-2
▪ Divide result by 2	11	-1
▪ Subtract original number	**6**	-1 - (-7)=**6**

Trick- solved

Choose any number:

Now double that number:

Add 12: + 12

Divide by 2: + 6

Subtract the original number: 6

Notice that our box is **PARTICULAR** because it represents a single quantity.

But our box is also **GENERIC** because any number whatsoever can be put in it.

Method of Direct Proof

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Lets use Direct Proofs!

Proof: the sum of any two even integers is even.

Formal Restatement: $\forall m,n \in \mathbf{Z}$. Even(m) $\wedge$ Even(n) $\rightarrow$ Even($m + n$)

Starting Point: Suppose m and n are *[pb.a.c]* even integers

particular **b**ut **a**rbitrarily **c**hosen

We need to Show that: $m+n$ is even

$m = 2k$
$n = 2j$
$m+n = 2k + 2j = 2(k+j)$
$(k+j)$ is integer
Thus: $2(k+j)$ is even

[This is what we needed to show.]

Theorem 4.1.1

Theorem 4.1.1

The sum of any two even integers is even.

Proof:

Suppose m and n are *[particular but arbitrarily chosen]* even integers. *[We must show that $m+n$ is even.]* By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$\begin{aligned} m+n &= 2r+2s && \text{by substitution} \\ &= 2(r+s) && \text{by factoring out a 2.} \end{aligned}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m+n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m+n$ is even. *[This is what we needed to show.]*†

Let's Use Direct Proofs!

Proof: the sum of an even integer plus an odd integer is always odd

What is a formal version (with a quantifier and variables) of this statement?

$\forall$ integers x and y, if x is even and y is odd, then $x + y$ is odd.

Outline of a Direct Proof

Write the first sentence (the "starting point") and the last sentence (the "conclusion to be shown") for a proof of the following statement:

$\forall$ integers x and y, if x is even and y is odd, then $x + y$ is odd.

Starting point:

Suppose x and y are any *[p.b.a.c.]* integers such that x is even and y is odd.

Conclusion to be shown: $x + y$ is odd.

See page 137

Prove: $\forall$ integers x and y, if x is even and y is odd, then $x+y$ is odd.

Proof: Suppose x and y are any *[particular but arbitrarily chosen]* integers such that x is even and y is odd.

[We must show that $x + y$ is odd.]

By definition of even and odd,

$x = 2a$ and $y = 2b + 1$ for some integers a and b.

Then

$$x + y = 2a + (2b+1) \quad \text{by substitution}$$
$$= 2(a + b) + 1 \quad \text{by algebra.}$$

Let $t = a + b$.

Then t is an integer because it is a sum of integers.

Hence $x + y = 2t + 1$, where t is an integer,

and thus by definition of odd,

goal → $x + y$ is odd.

[This is what we needed to show, and so we are done.]

QED

There are other okay ways to write this proof!

QED stands for *quod erat demonstrandum*, Latin for "which was to be shown."

Class Exercise

Proof: If k is an integer, is $2k - 1$ an odd integer?

Formally: $\forall k \in R$. Integer(k) $\rightarrow$ Odd(2k-1)

Starting Point: Suppose k is [p.b.a.c] integer

We need to Show that: *2k-1 is odd*

but 2k – 1 can be written as

$$2k–1+2-2 = 2k – 2 + 1$$
$$= 2(k – 1)+1$$

(k-1) is integer

Thus: 2(k-1) +1 is odd

[This is what we needed to show.]

Try by yourself

1. Prove that $10nm + 7$ is odd $\forall n, m \in \mathbb{Z}$.

How do start?

$\forall m,n$. if $m,n \in Z$ then $10mn+7$ is odd

2. Prove that

$\forall m, n \in \mathbb{Z}$, if $m > n > 0$ then is $m^2 - n^2$ composite?

3. How would you prove the following?

If x and y are two integers whose product is odd, then both must be odd.

Contraposition?

Directions for Writing Proofs for a Universal Statement

1. Copy the statement of the theorem to be proved onto your paper.
2. Clearly mark the beginning of your proof with the word "Proof."
3. Write your proof in complete sentences.
4. Make your proof self-contained. *(E.g., introduce all variables)*
5. Give a reason for each assertion in your proof.
6. Include the "little words" that make the logic of your arguments clear. *(E.g., then, thus, therefore, so, hence, because, since, Notice that, etc.)*
7. Make use of definitions but do not include them verbatim in the body of your proof.

Common Proof-Writing Mistakes

1. Arguing from examples.

Here is an example of this mistake. It is an incorrect "proof" of the fact that the sum of any two even integers is even. (Theorem 4.1.1).

> This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even.

2. Using the same letter to mean two different things.

Suppose m and n are any odd integers. Then by definition of odd, $m = 2k + 1$ and $n = 2k + 1$ for some integer k.

3. Jumping to a conclusion.

Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$. So $m + n$ is even.

4. Circular reasoning.

Suppose m and n are any odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.

Disproof a Universal Statement:

To disprove a statement means to show that the statement is false.
What do you have to do to show that this statement is false?

Answer: Show that the **negation** of the statement is **true**.

Most Common Method: Find a counterexample!

Example

Is the following statement true or false? Explain.

∀ real numbers x, if $x^2 > 25$ then $x > 5$.

Solution: The statement is false.

Counterexample:

Let $x = -6$. **Then** $x^2 = (-6)^2 = 36$, and $36 > 25$ **but** x 5.

So (for this x), $x^2 > 25$ and x 5.

Example: Disproof by Counterexample

Disprove the following statement:

$$\forall\ a, b \in R\ .\ a^2 = b^2 \rightarrow a = b.$$

Counterexample:

Let a = 1 and b = -1. **Then** $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$.
But $a \neq b$ since $1 \neq -1$.

Disproving an Existential Statement

Show that the following statement is false:
There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution Proving that the given statement is false is equivalent to proving its negation is true. The negation is:
For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is **universal**, it is proved by generalizing from the generic particular.
Claim: The statement "There is a positive integer n such that n2 + 3n + 2 is prime" is false.
Proof:

Suppose n is any *[particular but arbitrarily chosen]* positive integer. *[We will show that $n^2 + 3n + 2$ is not prime.]* We can factor $n^2 + 3n + 2$ to obtain $n^2 + 3n + 2 = (n + 1)(n + 2)$. We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$). Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime. ■